BOLETÍN DE ALERTA

Boletín Nro.: 2022-07

Fecha de publicación: 01/02/2022

Tema: Múltiples vulnerabilidades críticas en Samba

Software afectado:

- **Samba en sus versiones 4.0.0 a 4.13.16, 4.14.0 a 4.14.11 y 4.15.0 a 4.15.4.**

Descripción:

Samba ha publicado parches de seguridad para mitigar múltiples vulnerabilidades, entre ellas una de las más resaltantes que podría ocasionar ejecución remota de código (RCE) en el sistema afectado.

Las vulnerabilidades confirmadas se componen de 1 (una) vulnerabilidad *"Crítica"*, 1 (una) vulnerabilidad *"Alta"* y 1 (una) vulnerabilidad *"Media"* y se encuentran identificados como CVE-2021-44142, CVE-2022-0336 y CVE-2021-44141. Las mismas se detallan a continuación:

- CVE-2021-44142 de severidad critica, con una puntuación de 9.9. Esta vulnerabilidad se debe a una falla de programación en la lectura y escritura del *heap* de memoria, esto es debido a un error de límite al procesar los metadatos de *EA* al abrir archivos de *SMBD* dentro del módulo *VFS Samba* (*vfs_fruit*). Un atacante podría explotar esta vulnerabilidad y realizar ejecución remota de código (RCE) en el sistema afectado.

- CVE-2022-0336 de severidad alta, con una puntuación de 8.8. Esta vulnerabilidad se debe a que Samba AD DC incluye comprobaciones al agregar nombres de entidades principales de servicio (SPN) a una cuenta para garantizar que los SPN no coincidan con los que se encuentran en la base de datos. Algunas de estas comprobaciones se pueden evadir si en una modificación de cuenta se vuelve a agregar un SPN que estaba presente anteriormente en dicha cuenta. Un atacante podría aprovechar esta vulnerabilidad para realizar un ataque de denegación de servicio (DoS).

- CVE-2021-44141 de severidad media, con una puntuación de 4.2. Esta vulnerabilidad se debe a un fallo en los *symlinks* que permitirían la fuga de información de archivos o directorios fuera del recurso compartido. Un atacante podría aprovechar esta vulnerabilidad para así obtener información sobre los nombres de usuarios o el sistema operativo exacto, como así también de las aplicaciones que se ejecutan en el sistema afectado.

Ya existen varias PoC (pruebas de conceptos) publicadas disponibles en la red esto podría con llevar a la publicación de exploits prontamente, recomendamos la actualización de los servicios Samba los más pronto posible.

Impacto:

Un atacante podría realizar ejecución remota de código (RCE), denegación de servicio (DoS) o podría haber fuga de información de los sistemas de Samba afectados.

Solución:

Recomendamos instalar las actualizaciones de seguridad correspondientes al producto Samba utilizado afectado a través del siguiente enlace:

- https://www.samba.org/samba/security/

Información adicional:

- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-samba-2
- https://thehackernews.com/2022/01/new-samba-bug-allows-remote-attackers.html?m=1
- https://www.samba.org/samba/security/CVE-2021-44141.html
- https://www.samba.org/samba/security/CVE-2021-44142.html
- https://www.samba.org/samba/security/CVE-2022-0336.html
- https://www.cybersecurity-help.cz/vdb/SB2022013111